UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/620,817	07/16/2003	Stephen F. Bisbee	003670-104	1237

7590 07/18/2006

Burns, Doane, Swecker & Mathis, L.L.P.
P.O. Box 1404
Alexandria, VA 22313-1404

EXAMINER	
LOVING, JARIC E	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 07/18/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/620,817	BISBEE ET AL.	
	Examiner	Art Unit	
	Jaric Loving	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 July 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 July 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *12/19/03,9/23/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Information Disclosure Statement

1. The information disclosure statement contains non-patent literature ("NPL") documents that were not considered because they were not provided with the application. Furthermore, applicant refers to application 09/839,551 as a basis to refrain from providing the relevant NPL documents. However, applicant did not claim priority to that document and therefore, the NPL documents cited should have been provided.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-15, 19, 22-24, and 26-33 are rejected under 35 U.S.C. 102(e) as being anticipated by Koehler, US 6,301,658.

In claim 1, Koehler discloses a method of providing a Certificate Status Service ("CSS") for checking validities of authentication certificates issued by respective issuing Certification Authorities ("CAs"), comprising the steps of:

identifying information needed for retrieving a status of an authentication certificate from an issuing CA that issued the authentication certificate (col. 5, lines 14-20);

configuring a connector based on the identified information for communicating with the issuing CA (col. 5, lines 46-50);

communicating with the issuing CA according to the configured connector when the status of the authentication certificate is queried (col. 5, lines 53-55); and

retrieving the status of the authentication certificate (col. 5, lines 53-55; col. 6, lines 1-3);

wherein the issuing CA and the connector are designated on a list of approved CAs in a configuration store (col. 6, lines 3-8).

In claim 2, Koehler discloses the method of claim 1, wherein a local date and time are checked for whether they fall within a validity period indicated in the authentication certificate (col. 5, line 65 – col. 6,line 3).

In claim 3, Koehler discloses the method of claim 1, wherein the issuing CA is included in the list of approved CAs by vetting and approving the issuing CA according to predetermined business rules, and if the issuing CA is vetted and not approved, the issuing CA is designated on a list of not-approved CAs in the configuration store (col. 5, lines 21-36; col. 8, lines 16-21).

In claim 4, Koehler discloses the method of claim 3, wherein vetting and approving the issuing CA includes registering a representation of a trusted authentication certificate with the CSS and adding at least the representation, status and a time-to-live data element to a local cache memory, and a connector is configured for retrieving the added status when the status of the trusted authentication certificate is queried (col. 7, lines 12-16 – timestamp provides a time to live; col. 8, lines 21-36).

In claim 5, Koehler discloses the method of claim 2, further comprising the steps of checking a local cache memory for the status, and if the status is found in the local cache memory and the local date and time are within the validity period, retrieving the status from the local cache memory, wherein if the status is not found in the local cache memory or if the local date and time are not within the validity period, the CSS establishes a communication session with a certificate status reporting component of the issuing CA, composes a certificate status request according to the configured connector, retrieves the status from the certificate status reporting component, closes the communication session with certificate status reporting component, and adds at least the authentication certificate's identification, status, and time-to-live to the local cache memory (col. 5, line 65 – col. 6, line 27).

In claim 6, Koehler discloses the method of claim 1, wherein the certificate status is indicated by a Certificate Revocation List (CRL), according to a publication schedule of the issuing CA, the CSS retrieves the CRL from a certificate status reporting component listed in the configuration store, the CSS clears a cache memory associated with the issuing CA, and the CSS determines the status of the authentication certificate from the CRL and stores the status in the cache memory associated with the issuing CA (col. 5, line 65 – col. 6, line 27 – verification server can also consider CRL of CA).

In claim 7, Koehler discloses the method of claim 1, wherein the certificate status is indicated by a Delta Certificate Revocation List ("ΔCRL"); upon notification by the issuing CA that a ΔCRL is available, the CSS retrieves the ΔCRL from a certificate status reporting component listed in the configuration store; if the ΔCRL is a complete

CRL, then the CSS clears a cache memory associated with the issuing CA, determines the status from the CRL, and stores the status in the cache memory; and if the ΔCRL contains only changes occurring after publication of a full CRL, the CSS determines the status from the ΔCRL, and stores the status in the cache memory (col. 7, lines 12-34).

In claim 8, Koehler discloses the method of claim 1, wherein the communicating step includes communicating according to a sequence of connectors (col. 5, lines 42-46; col. 8, lines 37-45).

In claim 9, Koehler discloses the method of claim 1, wherein a connector embeds more than one certificate status check in a single communicating step (col. 5, lines 42-46; col. 8, lines 37-45).

In claim 10, Koehler discloses the method of claim 1, wherein the authentication certificate is not used for identification (col. 5, lines 42-46; col. 8, lines 37-45).

In claim 11, Koehler discloses a method of retrieving a status of an authentication certificate issued by an issuing Certification Authority ("CA") in response to a query from a Trusted Custodial Utility ("TCU") to a Certificate Status Service ("CSS") to validate the authentication certificate's status, comprising the steps of:

locating and reporting the status if the status is present and current in a cache memory of the CSS (col. ,line 63 – col. 6, line 8);

otherwise performing the steps of:

obtaining a status type and retrieval method from a CSS configuration store (col. ,line 63 – col. 6, line 8);

if the status type is Certificate Revocation List ("CRL") and the status is not found in the cache memory, then reporting the status as valid (col. 6, lines 9-27);

if the status type is not CRL, then composing a certificate status request according to the status type (col. 6, lines 9-27 – if no entry, status composed from repository);

establishing a communication session with the issuing CA (col. 5, lines 48-55; col. 6, lines 28-41);

retrieving the status from a status reporting component of the issuing CA using the obtained retrieval method and ending the communication session (col. 6, lines 56-66);

interpreting the retrieved status (col. 6, lines 56-66);

associating, with the interpreted retrieved status, a time-to-live value representing a period specified by a CSS policy for the status type (col. 6, lines 56-66);

adding at least the authentication certificate's identification, status, and time-to-live values to the cache memory (col. 5, line 63 – col. 6, line 8); and

reporting the status to the TCU in response to the query (col. 8, lines 2-21).

In claim 12, Koehler discloses the method of claim 11, wherein the CSS uses a certificate status protocol in the communication session (col. 5, lines 44-48).

In claim 13, Koehler discloses the method of claim 11, wherein more than one status is retrieved using the obtained retrieval method (col. 5, lines 42-48).

In claim 14, Koehler discloses the method of claim 11, wherein the authentication certificate is not used for identification (col. 5, lines 42-46; col. 8, lines 37-45).

In claim 15, Koehler discloses a Certificate Status Service ("CSS") for providing accurate and timely status indications of authentication certificates issued by issuing Certification Authorities ("CAs"), comprising:

providing a status of an authentication certificate as indicated by a Certificate Revocation List ("CRL") when the certificate's issuing CA uses CRLs for indicating status (col. 7, lines 12-34);

otherwise, providing the status indicated by a cache memory when the cache memory includes a status and a time-to-live data element is not exceeded (col. 7, lines 17-19);

if the time-to-live data element is exceeded, clearing the status from the cache memory (col. 5, lines 47-49);

requesting and retrieving the status using a real-time certificate status reporting protocol when the status is not in the cache memory (col. 5, lines 53-55);

adding at least the certificate's identification, status, and time-to-live data element to the cache memory (col. 5, line 63 – col. 6, line 8); and

providing the retrieved status (col. 5, line 63 – col. 6, line 8).

In claim 19, Koehler discloses a method of executing a transaction between a first party and a second party by transferring control of an authenticated information object having a verifiable evidence trail, comprising the steps of:

retrieving an authenticated information object from a trusted repository, wherein the authenticated information object includes a first digital signature block comprising a digital signature of a submitting party and a first authentication certificate relating at

least an identity and a cryptographic key to the submitting party, a date and time indicator, and a second digital signature block comprising a second digital signature of the trusted repository and a second authentication certificate relating at least an identity and a cryptographic key to the trusted repository; the first digital signature block was validated by the trusted repository; and the authenticated information object is stored as an electronic original information object under the control of the trusted repository (col. 7, line 66 – col. 8, line 21 – root has authentication authority of other CAs);

executing the retrieved authenticated information object by the second party by including in the retrieved authenticated information object a third digital signature block comprising at least a third digital signature and a third authentication certificate of the second party (col. 7, line 66 – col. 8, line 21); and

forwarding the executed retrieved authenticated information object to a trusted custodial utility ("TCU"), wherein the TCU verifies digital signatures and validates authentication certificates associated with the digital signatures included in information objects by at least retrieving status of the authentication certificates from a Certificate Status Service ("CSS") provided according to claim 1; the TCU rejects a digital signature block if the respective digital signature is not verified or the status of the respective authentication certificate is expired or is revoked; and if at least one signature block in the information object is not rejected, the TCU appends the TCU's digital signature block and a date and time indicator to the information object and takes control of the object on behalf of the first party (col.5 ,lines 53-55; col. 5, line 63 – col. 6, line 8; col. 7, line 66 – col. 8, line 21).

In claim 22, Koehler discloses the method of claim 19, wherein if the TCU rejects a digital signature block, the TCU requests a remedy that requires the digital signature to be recomputed and the signature block to be reforwarded (col. 6, lines 33-51).

In claim 23, Koehler discloses the method of claim 19, wherein the TCU checks the local date and time for accuracy and that they are within a validity period indicated by the second party's authentication certificate (col. 6, lines 33-51 – root CA checks timestamp).

In claim 24, Koehler discloses the method of claim 23, wherein if the local date and time are not within the validity period indicated by the second party's authentication certificate, the TCU notifies the second party that the authentication certificate is rejected and the first party that the transaction is incomplete (col. 6, lines 30-33).

In claim 26, Koehler discloses the method of claim 19, wherein one or more digitized handwritten signatures are included in the information object, and placement of the digitized handwritten signatures in a data structure is specified by at least one signature tag (col. 4, line 66 – col. 5, line 20).

In claim 27, Koehler discloses the method of claim 26, wherein one or more signature blocks are separately forwarded to the TCU with respective signature tags, and the TCU validates the signature blocks by:

rejecting a signature block if either the respective digital signature is not verified or the respective authentication certificate is not validated (col. 5, lines 27-29; col. 5, line 63 – col. 6, line 8), and

placing the signature block according to the respective signature tag if the signature block is not rejected (col. 5, lines 2-20 – timestamp is entered according to whether it is expired, also public keys are entered based on validity),

wherein, to signature blocks sent separately, the TCU adds a date and time indication to each signature block and appends according to business rules the TCU's signature block in a wrapper that encompasses the information object and placed signature blocks (col. 5, line 63 – col. 6, line 3).

In claim 28, Koehler discloses the method of claim 27, wherein the TCU verifies a digital signature and validates an authentication certificate in a signature block by:

determining from the business rules whether a party associated with the authentication certificate has authority (col. 5, lines 14-15),

verifying the party's digital signature, checking that the authentication certificate's validity period overlaps the TCU's current date and time (col. 5, lines 17-20),

checking that the local date and time falls within an allowable deviation from the TCU's current date and time (col. 5, lines 8-10), and

retrieving status of the authentication certificate from the CSS (col. 5, line 63 – col. 6, line 3), and

if any of the preceding steps results in an invalid or false output, the digital signature is deemed invalid, the transaction is not executed, otherwise the digital signature is deemed valid and the transaction is executed (col. 6, lines 28-51).

In claim 29, Koehler discloses the method of claim 19, wherein the CSS provides authentication certificate status to the TCU by at least the steps of checking a local

cache memory for the status, and if the status is found in the local cache memory and the local date and time are within the validity period, and retrieving the status from the local cache memory; if the status is not found in the local cache memory or if the local date and time are not within the validity period, the CSS establishes a communication session with a certificate status reporting component of the issuing CA, composes a certificate status request according to the configured connector, retrieves the status from the certificate status reporting component, closes the communication session with certificate status reporting component, and adds at least the authentication certificate's identification, status, and a time-to-live data element to the local cache memory (col. 5, lines 48-55; col. 5, line 65 – col. 6, line 8).

In claim 30, Koehler discloses the method of claim 19, wherein the first party is a first TCU and the transaction is for transferring custody of one or more electronic originals to the first TCU from a second TCU, an owner of the transaction provides the second TCU with a manifest that identifies electronic originals to be transferred to the first TCU, the second TCU establishes communication with the first TCU and identifies the purpose of its actions, the manifest is communicated to the first TCU so that it is able to determine when the transfer of custody has been completed, the second TCU transfers each identified electronic original to the first TCU, the first TCU retrieves status of the second TCU's certificate and verifies the second TCU's digital signature on each transferred electronic original, if any of the second TCU's digital signatures or certificates are invalid, then the first TCU notifies the second TCU and seeks a remedy, if the second TCU does not provide a remedy, the first TCU notifies the transaction

owner that the requested transfer of custody has failed, otherwise the second TCU creates a new wrapper for each successfully transferred information object, adding a date-time stamp and the first TCU's signature block (col. 6, lines 28-55; col. 8, lines 2-36).

In claim 31, Koehler discloses the method of claim 30, wherein the transaction is a transfer of ownership in response to an instruction, transfer of ownership documentation is placed in either the first TCU or the second TCU, the TCU having the transfer of ownership documentation validates authenticity of the transfer of ownership documentation by verifying all digital signatures, certificate validity periods, and using the CSS to check certificate status of all authentication certificates included in the transfer of ownership documentation, appends a date and time indication, and digitally signs, wraps and stores the transfer of ownership documentation, which are added to the manifest (col. 6, lines 28-55; col. 8, lines 2-36).

In claim 32, Koehler discloses the method of claim 19, wherein the certificate status is indicated by a Certificate Revocation List (CRL), according to a publication schedule of the issuing CA, the CSS retrieves the CRL from a certificate status reporting component listed in the configuration store, the CSS clears a cache memory associated with the issuing CA, and the CSS determines the status of the authentication certificate from the CRL and stores the status in the cache memory associated with the issuing CA (col. 5, line 65 – col. 6, line 27).

In claim 33, Koehler discloses the method of claim 19, wherein the certificate status is indicated by a Delta Certificate Revocation List ("ΔCRL"); upon notification by

the issuing CA that a ΔCRL is available, the CSS retrieves the ΔCRL from a certificate status reporting component listed in the configuration store; if the ΔCRL is a complete CRL, then the CSS clears a cache memory associated with the issuing CA, determines the status from the CRL, and stores the status in the cache memory; and if the ΔCRL contains only changes occurring after publication of a full CRL, the CSS determines the status from the ΔCRL, and stores the status in the cache memory (col. 7, lines 12-34).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 16-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Koehler and further in view of Konheim, US 4,264,782.

In claim 16, Koehler fails to disclose a status use-counter data element is added to the cache memory; the status use-counter data element is incremented or decremented every time the certificate's status is checked; and if the status use-counter data element passes a threshold, then the status is provided and the cache memory is cleared with respect to the status. Konheim discloses a status use-counter data element is added to the cache memory; the status use-counter data element is incremented or decremented every time the certificate's status is checked; and if the status use-counter data element passes a threshold, then the status is provided and the

cache memory is cleared with respect to the status (col. 11, lines 58-68; col. 12, lines 37-47).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Koehler's digital certificate authentication system with Konheim's identity verification method utilizing a use-counter to check memory access. It is for this reason that one of ordinary skill in the art would have been motivated to provide Koehler's digital certificate authentication system with a use-counter because it protects against the re-use of a previously verified transaction (Konheim, col. 7, lines 4-6).

In claim 17, Koehler, as modified, discloses the CSS of claim 16, wherein a status last-accessed data element is added to the cache memory, and the status last-accessed data element in conjunction with the status use-counter data element enable determination of an activity level of the certificate's status (Koehler, col. 6, lines 17-22).

In claim 18, Koehler, as modified, discloses the CSS of claim 17, wherein when a request is made to the CSS to retrieve a status of a new certificate and the cache memory has reached an allocated buffer size limit, the CSS searches the cache memory for a lasted-accessed data element indicating an oldest date and clears the respective cache memory entry; and the CSS then retrieves the requested status, places it in the cache memory, and provides the requested status (col. 6, lines 12-27; col. 7, lines 52-57 – updates timestamp which thus clears the memory and enters a new value).

5. Claims 20-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Koehler and further in view of Kocher, US 5,903,651.

In claim 20, Koehler fails to disclose a signature block including at least one hash of at least a portion of the information object in which the signature block is included, the at least one hash is encrypted by the cryptographic key of the block's respective signer, thereby forming the signer's digital signature, and the signer's digital signature is included in the signature block with the signer's authentication certificate. Kocher discloses a signature block including at least one hash of at least a portion of the information object in which the signature block is included, the at least one hash is encrypted by the cryptographic key of the block's respective signer, thereby forming the signer's digital signature, and the signer's digital signature is included in the signature block with the signer's authentication certificate (col. 4, lines 23-26 and lines 41-45).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Koehler's digital certificate authentication system with Kocher's method of confirming certificate status utilizing hashing a portion of information to create more secure data transfers. It is for this reason that one of ordinary skill in the art would have been motivated to provide Koehler's digital certificate authentication system with hashing because it allows certificate status to be determined without knowledge of an entire list of revoked certificates (Kocher, col. 3, lines 29-32 and lines 59-61).

In claim 21, Koheler, as modified, discloses the method of claim 20, wherein the executing step includes displaying a local date and time to the second party, affirming, by the second party, that the displayed local date and time are correct, and correcting the local date and time if either is incorrect (Koehler, col. 7, lines 43-57).

6. Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over Koehler and further in view of Smithies et al., US 5,818,955.

In claim 25, Koehler fails to disclose one or more digitized handwritten signatures are included in the information object, and placement of the digitized handwritten signatures in a data structure is specified by at least one signature tag. Smithies discloses one or more digitized handwritten signatures are included in the information object, and placement of the digitized handwritten signatures in a data structure is specified by at least one signature tag (col. 3, lines 39-49).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Koehler's digital certificate authentication system with Smithies signature verification method utilizing digitized handwritten signatures to allow a user to store a handwritten signature. It is for this reason that one of ordinary skill in the art would have been motivated to provide Koehler's digital authentication system with digitized handwritten signatures because it allows a person to determine whether two signatures are from the same person (Smithies, col. 3, lines 12-18).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jaric Loving whose telephone number is (571) 272-1686. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone

number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JL

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100